NETWORK
ENVIRONMENT

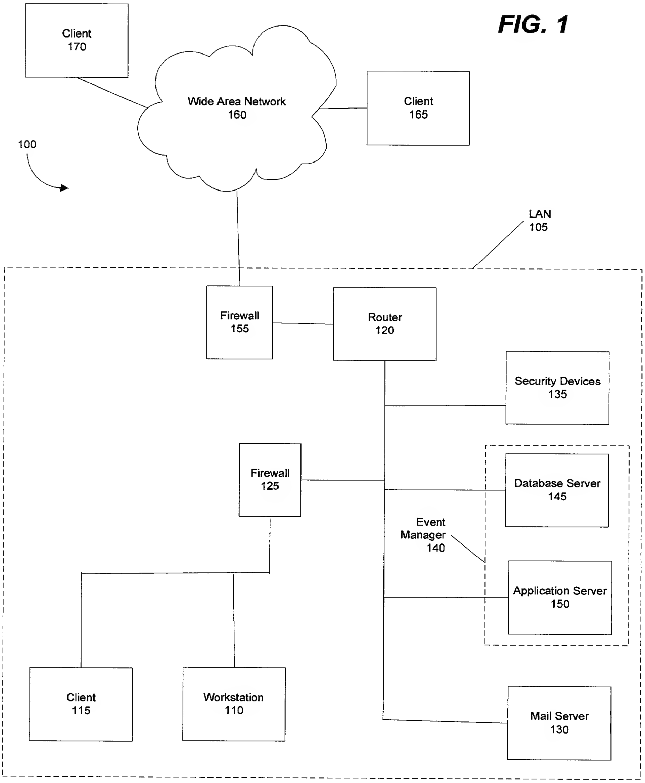


FIG. 1

ARCHITECTURE

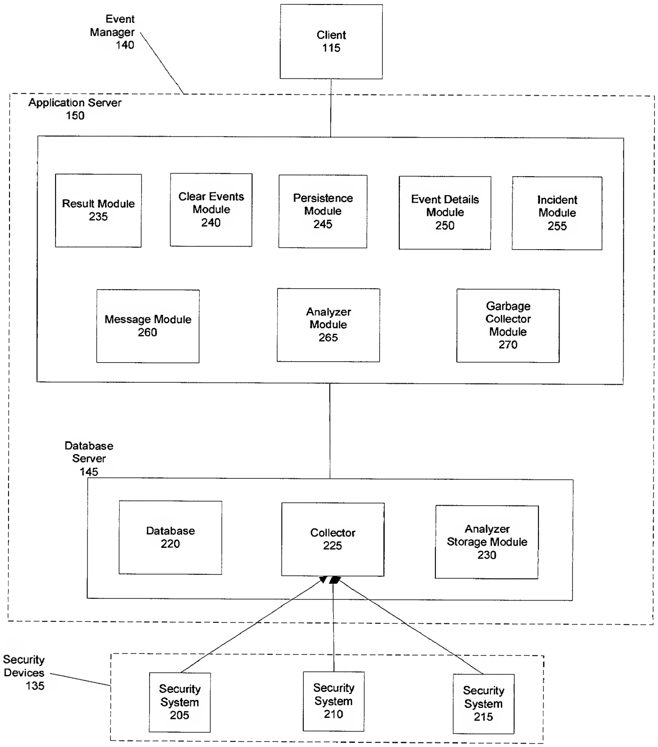


FIG. 2

OVERVIEW

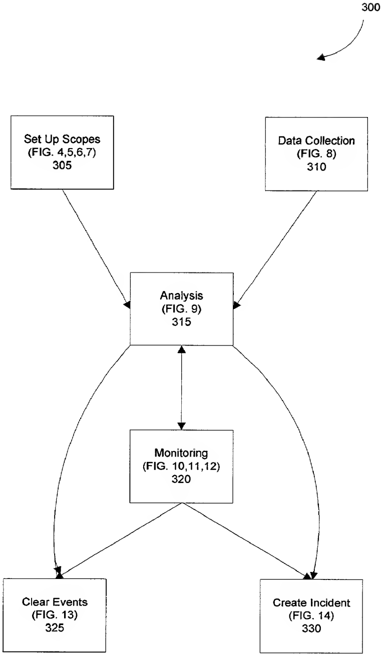


FIG. 3

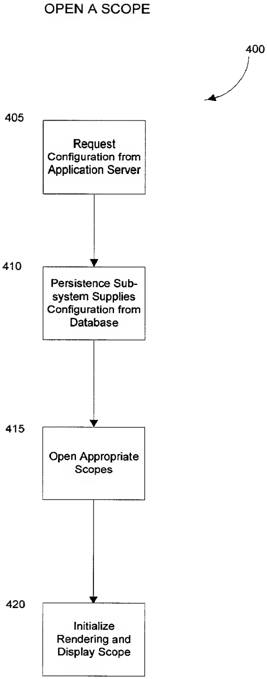

OPEN A SCOPE
400
405
Request Configuration from Application Server
410
Persistence Sub-system Supplies Configuration from Database
415
Open Appropriate Scopes
420
Initialize Rendering and Display Scope

FIG. 4

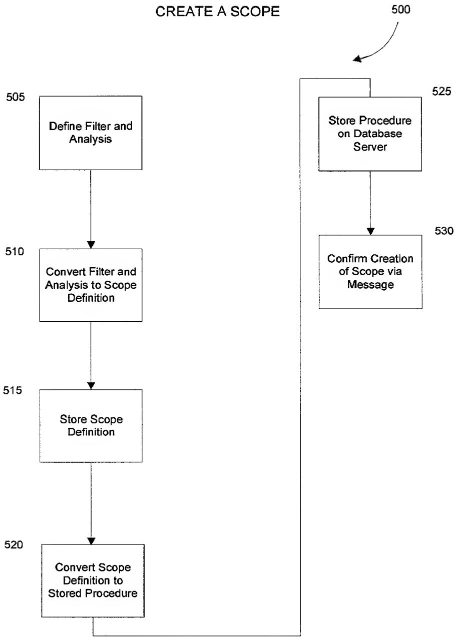

CREATE A SCOPE
500
505
Define Filter and Analysis
510
Convert Filter and Analysis to Scope Definition
515
Store Scope Definition
520
Convert Scope Definition to Stored Procedure
525
Store Procedure on Database Server
530
Confirm Creation of Scope via Message

FIG. 5

EDIT A SCOPE

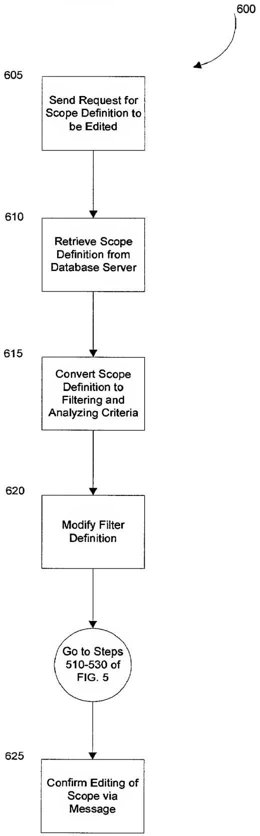

600
605
Send Request for Scope Definition to be Edited
610
Retrieve Scope Definition from Database Server
615
Convert Scope Definition to Filtering and Analyzing Criteria
620
Modify Filter Definition
Go to Steps 510-530 of FIG. 5
625
Confirm Editing of Scope via Message

FIG. 6

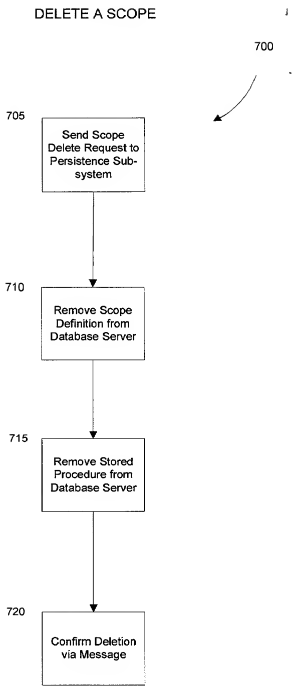

DELETE A SCOPE
700
705
Send Scope Delete Request to Persistence Sub-system
710
Remove Scope Definition from Database Server
715
Remove Stored Procedure from Database Server
720
Confirm Deletion via Message

FIG. 7

DATA COLLECTION

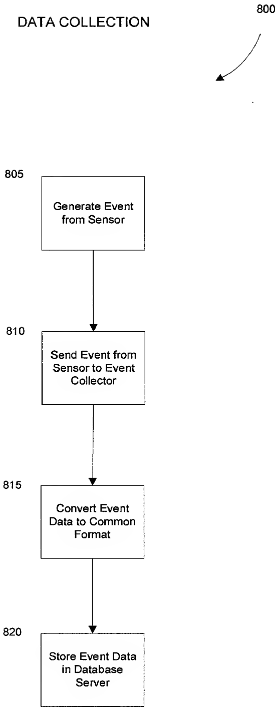

800
805
Generate Event from Sensor
810
Send Event from Sensor to Event Collector
815
Convert Event Data to Common Format
820
Store Event Data in Database Server

FIG. 8

ANALYSIS

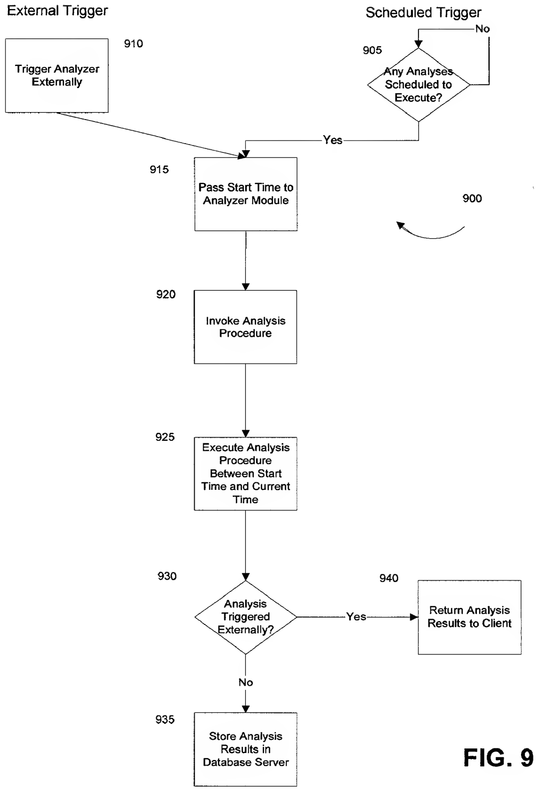

External Trigger
Scheduled Trigger
910
Trigger Analyzer Externally
905
Any Analyses Scheduled to Execute?
No
Yes
915
Pass Start Time to Analyzer Module
900
920
Invoke Analysis Procedure
925
Execute Analysis Procedure Between Start Time and Current Time
930
Analysis Triggered Externally?
Yes
940
Return Analysis Results to Client
No
935
Store Analysis Results in Database Server

FIG. 9

MONITORING/
POLLING FOR DATA

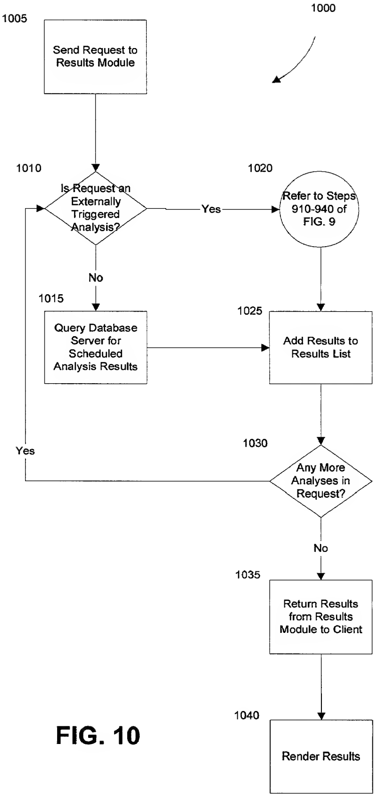

1000
1005
Send Request to Results Module
1010
Is Request an Externally Triggered Analysis?
Yes
1020
Refer to Steps 910-940 of FIG. 9
No
1015
Query Database Server for Scheduled Analysis Results
1025
Add Results to Results List
1030
Any More Analyses in Request?
Yes
No
1035
Return Results from Results Module to Client
1040
Render Results

FIG. 10

MONITORING/ POLLING FOR MESSAGES

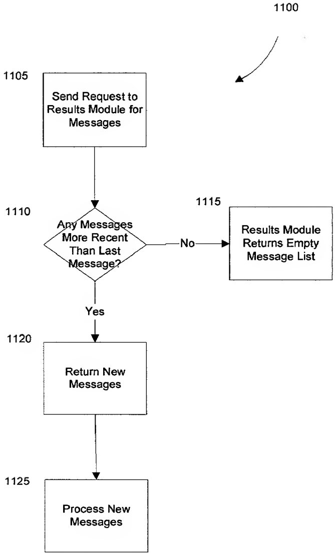

1100
1105
Send Request to Results Module for Messages
1110
Any Messages More Recent Than Last Message?
No
1115
Results Module Returns Empty Message List
Yes
1120
Return New Messages
1125
Process New Messages

FIG. 11

REQUESTING EVENT DETAILS

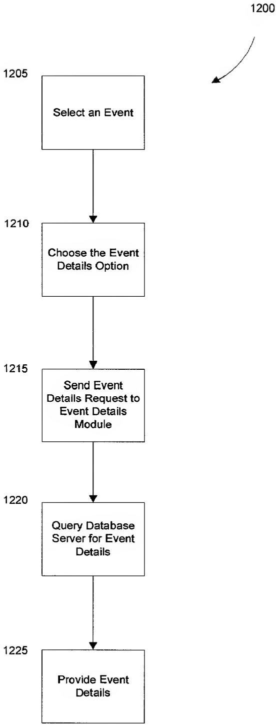

1200
1205
Select an Event
1210
Choose the Event Details Option
1215
Send Event Details Request to Event Details Module
1220
Query Database Server for Event Details
1225
Provide Event Details

FIG. 12

CLEAR AN EVENT

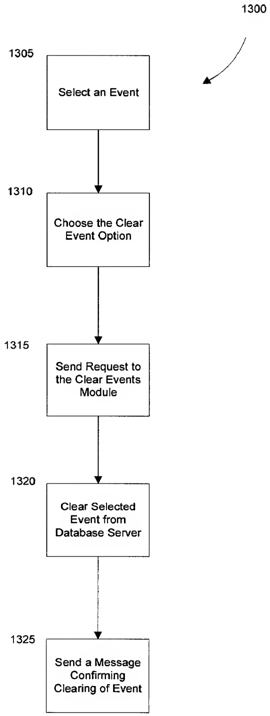

1300
1305
Select an Event
1310
Choose the Clear Event Option
1315
Send Request to the Clear Events Module
1320
Clear Selected Event from Database Server
1325
Send a Message Confirming Clearing of Event

FIG. 13

CREATE INCIDENT

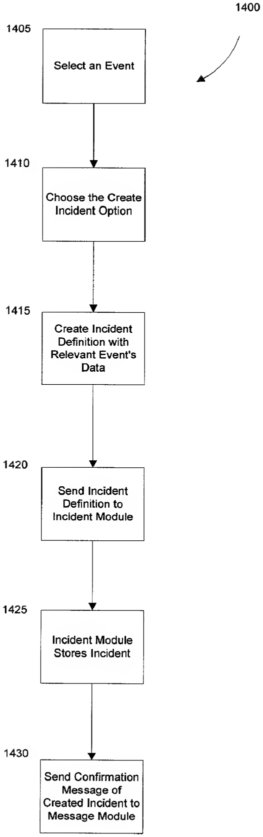
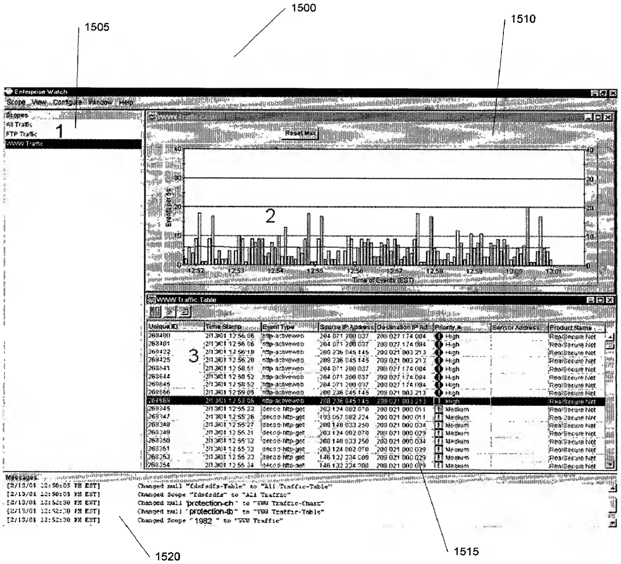

1400
1405
Select an Event
1410
Choose the Create Incident Option
1415
Create Incident Definition with Relevant Event's Data
1420
Send Incident Definition to Incident Module
1425
Incident Module Stores Incident
1430
Send Confirmation Message of Created Incident to Message Module

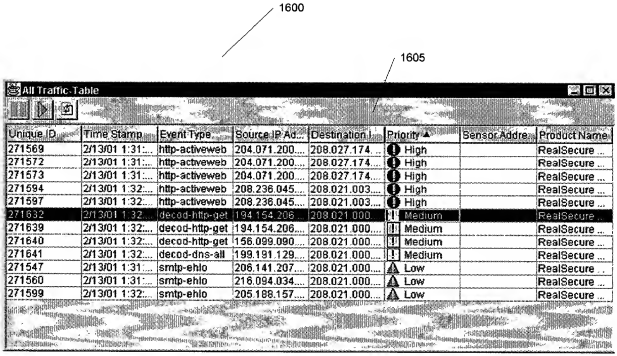
FIG. 14



Unique ID	Time Stamp	Event Type	Source IP Address	Destination IP Ad	Priority	Sensor Address	Product Name
268400	2/13/01 12:56:06	http-activeweb	204 071 200 037	208 027 174 084	● High		RealSecure Net
268401	2/13/01 12:56:06	http-activeweb	204 071 200 037	208 027 174 084	● High		RealSecure Net
269432	2/13/01 12:56:19	http-activeweb	208 236 045 145	208 021 003 213	● High		RealSecure Net
269425	2/13/01 12:56:20	http-activeweb	208 236 045 145	208 021 003 213	● High		RealSecure Net
268641	2/13/01 12:58:51	http-activeweb	204 071 200 037	208 027 174 084	● High		RealSecure Net
268644	2/13/01 12:58:52	http-activeweb	204 071 200 037	208 027 174 084	● High		RealSecure Net
269645	2/13/01 12:58:52	http-activeweb	204 071 200 037	208 027 174 084	● High		RealSecure Net
268666	2/13/01 12:59:05	http-activeweb	208 236 045 145	208 021 003 213	● High		RealSecure Net
268669	2/13/01 12:59:06	http-activeweb	208 236 045 145	208 021 003 213	High		RealSecure Net
268345	2/13/01 12:55:23	decod-http-get	203 124 002 070	208 021 000 011	! Medium		RealSecure Net
268347	2/13/01 12:55:26	decod-http-get	193 057 082 224	208 021 000 011	! Medium		RealSecure Net
268348	2/13/01 12:55:27	decod-http-get	208 140 033 250	208 021 000 034	! Medium		RealSecure Net
268349	2/13/01 12:55:31	decod-http-get	203 124 002 070	208 021 000 029	! Medium		RealSecure Net
268350	2/13/01 12:55:32	decod-http-get	208 140 033 250	208 021 000 034	! Medium		RealSecure Net
268351	2/13/01 12:55:32	decod-http-get	203 124 002 070	208 021 000 029	! Medium		RealSecure Net
268353	2/13/01 12:55:33	decod-http-get	146 132 234 209	208 021 000 029	! Medium		RealSecure Net
268354	2/13/01 12:55:34	decod-http-get	146 132 234 208	208 021 000 029	! Medium		RealSecure Net

```
[2/13/01 12:50:05 PM EST]          Changed null "fdsfsdfs-Table" to "All Traffic-Table"
[2/13/01 12:50:05 PM EST]          Changed Scope "fdsfsdfs" to "All Traffic"
[2/13/01 12:52:30 PM EST]          Changed null 'protection-ch " to "WWW Traffic-Chart"
[2/13/01 12:52:30 PM EST]          Changed null 'protection-tb" to "WWW Traffic-Table"
[2/13/01 12:52:30 PM EST]          Changed Scope "1982 " to "WWW Traffic"
```

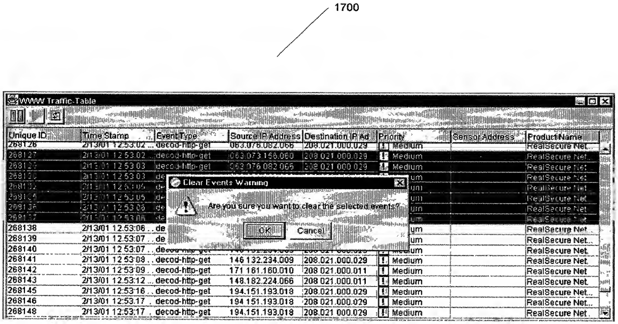
FIG. 15



All Traffic-Table

Unique ID	Time Stamp	Event Type	Source IP Ad...	Destination I...	Priority ▲	Sensor Addre...	Product Name
271569	2/13/01 1:31:...	http-activeweb	204.071.200....	208.027.174. ..	❗ High		RealSecure ...
271572	2/13/01 1:31:...	http-activeweb	204.071.200....	208.027.174....	❗ High		RealSecure ...
271573	2/13/01 1:31:...	http-activeweb	204.071.200....	208.027.174....	❗ High		RealSecure ...
271594	2/13/01 1:32:...	http-activeweb	208.236.045....	208.021.003....	❗ High		RealSecure ...
271597	2/13/01 1:32:...	http-activeweb	208.236.045....	208.021.003....	❗ High		RealSecure ...
271632	2/13/01 1:32:...	decod-http-get	194.154.206....	208.021.000....	! Medium		RealSecure ...
271639	2/13/01 1:32:...	decod-http-get	194.154.206....	208.021.000....	! Medium		RealSecure ...
271640	2/13/01 1:32:...	decod-http-get	156.099.090....	208.021.000....	! Medium		RealSecure ...
271641	2/13/01 1:32:...	decod-dns-all	199.191.129....	208.021.000....	! Medium		RealSecure ...
271547	2/13/01 1:31:...	smtp-ehlo	206.141.207....	208.021.000....	⚠ Low		RealSecure ...
271560	2/13/01 1:31:...	smtp-ehlo	216.094.034....	208.021.000....	⚠ Low		RealSecure ...
271599	2/13/01 1:32:...	smtp-ehlo	205.188.157....	208.021.000....	⚠ Low		RealSecure ...

FIG. 16



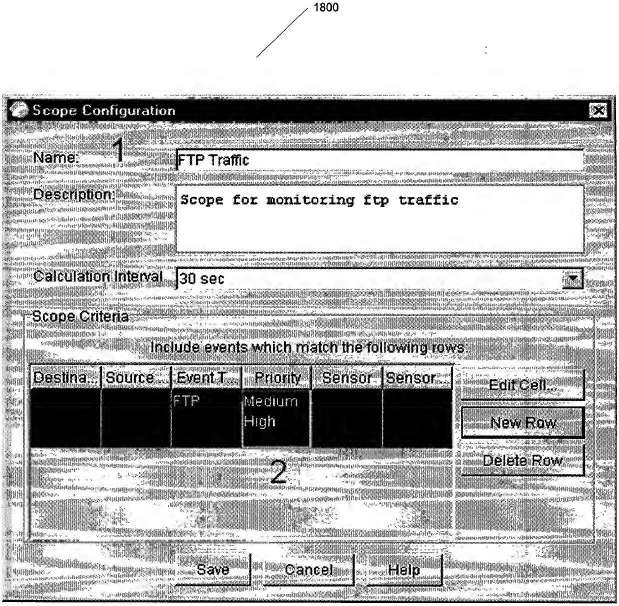
WWW Traffic-Table

Unique ID	Time Stamp	Event Type	Source IP Address	Destination IP Ad	Priority	Sensor Address	Product Name
268126	2/13/01 12:53:02 ...	decod-http-get	063.076.082.066	208.021.000.029	! Medium		RealSecure Net...
268127	2/13/01 12:53:02 ...	decod-http-get	063.073.156.060	208.021.000.029	! Medium		RealSecure Net...
268128	2/13/01 12:53:03	decod-http-get	063.076.082.065	208.021.000.029	! Medium		RealSecure Net
268130	2/13/01 12:53:03	de			um		RealSecure Net
268132	2/13/01 12:53:05	de			um		RealSecure Net
268134	2/13/01 12:53:05	de			um		RealSecure Net
268136	2/13/01 12:53:06	de			um		RealSecure Net
268137	2/13/01 12:53:06	de			um		RealSecure Net
268138	2/13/01 12:53:06 ..	de			um		RealSecure Net...
268139	2/13/01 12:53:07 ..	de			um		RealSecure Net...
268140	2/13/01 12:53:07 ..	decod-http-get			Medium		RealSecure Net.
268141	2/13/01 12:53:08 ..	decod-http-get	146.132.234.009	208.021.000.029	! Medium		RealSecure Net.
268142	2/13/01 12:53:09 ..	decod-http-get	171.161.160.010	208.021.000.011	! Medium		RealSecure Net
268143	2/13/01 12:53:12 ...	decod-http-get	148.182.224.066	208.021.000.011	! Medium		RealSecure Net.
268145	2/13/01 12:53:16 ..	decod-http-get	194.151.193.018	208.021.000.029	! Medium		RealSecure Net...
268146	2/13/01 12:53:17 .	decod-http-get	194.151.193.018	208.021.000.029	! Medium		RealSecure Net...
268148	2/13/01 12:53:17 .	decod-http-get	194.151.193.018	208.021.000.029	! Medium		RealSecure Net.

Clear Events Warning

Are you sure you want to clear the selected events?

FIG. 17



Name: FTP Traffic

Description: Scope for monitoring ftp traffic

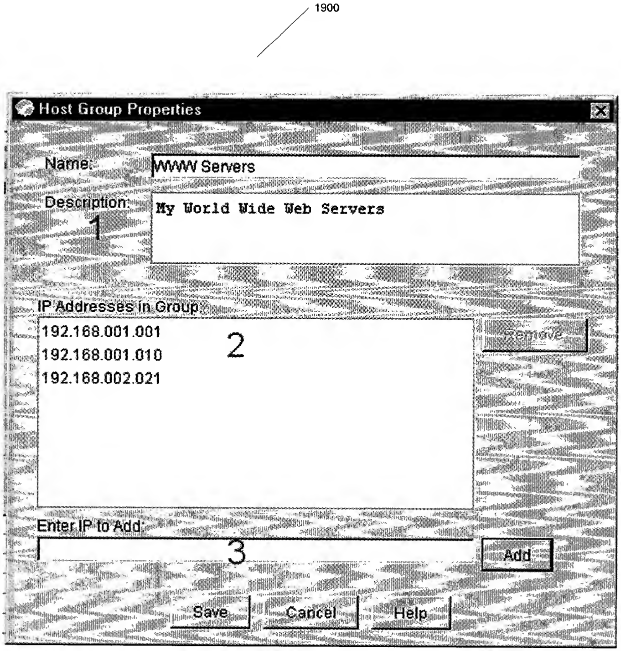
Calculation Interval 30 sec

Scope Criteria

Include events which match the following rows:

Destina...	Source ...	Event T...	Priority	Sensor	Sensor ...
		FTP	Medium High		

FIG. 18



Name: WWW Servers

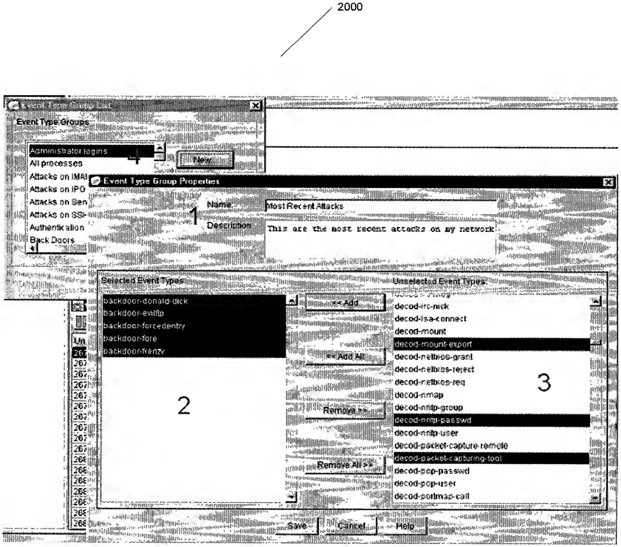
Description: My World Wide Web Servers

IP Addresses in Group:

192.168.001.001
192.168.001.010
192.168.002.021

Enter IP to Add:

FIG. 19



Event Type Groups

Administrator logins
All processes
Attacks on IMAI
Attacks on IPO
Attacks on Sen
Attacks on SSH
Authentication
Back Doors

Event Type Group Properties

Name: Most Recent Attacks

Description: This are the most recent attacks on my network

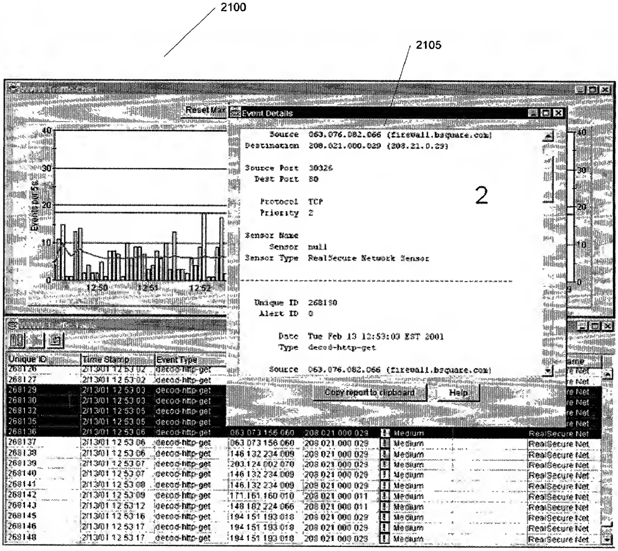
Selected Event Types

backdoor-donald-dick
backdoor-evilftp
backdoor-forcedentry
backdoor-fore
backdoor-frenzy

Unselected Event Types:

decod-irc-nick
decod-isa-connect
decod-mount
decod-mount-export
decod-netbios-grant
decod-netbios-reject
decod-netbios-req
decod-nmap
decod-nntp-group
decod-nntp-passwd
decod-nntp-user
decod-packet-capture-remote
decod-packet-capturing-tool
decod-pop-passwd
decod-pop-user
decod-portmap-call

FIG. 20



```
     Source  063.076.082.066 (firewall.bsquare.com)
Destination  208.021.000.029 (208.21.0.29)

Source Port  30326
  Dest Port  80

   Protocol  TCP
   Priority  2

Sensor Name
     Sensor  null
Sensor Type  RealSecure Network Sensor

-----------------------------------------------------

  Unique ID  268130
   Alert ID  0

       Date  Tue Feb 13 12:53:03 EST 2001
       Type  decod-http-get

     Source  063.076.082.066 (firewall.bsquare.com)
```

Unique ID	Time Stamp	Event Type					ame
268126	2/13/01 12 53 02	decod-http-get					re Net
268127	2/13/01 12 53 02	decod-http-get					re Net
268129	2/13/01 12 53 03	decod-http-get					re Net
268130	2/13/01 12 53 03	decod-http-get					re Net
268132	2/13/01 12 53 05	decod-http-get					re Net
268135	2/13/01 12 53 05	decod-http-get					re Net
268136	2/13/01 12 53 06	decod-http-get	063 073 156 060	208 021 000 029	!	Medium	RealSecure Net
268137	2/13/01 12 53 06	decod-http-get	063 073 156 060	208 021 000 029	!	Medium	RealSecure Net
268138	2/13/01 12 53 06	decod-http-get	146 132 234 009	208 021 000 029	!	Medium	RealSecure Net
268139	2/13/01 12 53 07	decod-http-get	203 124 002 070	208 021 000 029	!	Medium	RealSecure Net
268140	2/13/01 12 53 07	decod-http-get	146 132 234 009	208 021 000 029	!	Medium	RealSecure Net
268141	2/13/01 12 53 08	decod-http-get	146.132 234 009	208 021 000 029	!	Medium	RealSecure Net
268142	2/13/01 12 53 09	decod-http-get	171.161 160 010	208 021 000 011	!	Medium	RealSecure Net
268143	2/13/01 12 53 12	decod-http-get	148 182 224 066	208 021 000 011	!	Medium	RealSecure Net
268145	2/13/01 12 53 16	decod-http-get	194 151 193 018	208 021 000 029	!	Medium	RealSecure Net
268146	2/13/01 12 53 17	decod-http-get	194 151 193 018	208 021 000 029	!	Medium	RealSecure Net
268148	2/13/01 12 53 17	decod-http-get	194 151 193 018	208 021 000 029	!	Medium	RealSecure Net

FIG. 21